Quantum Codes and Symplectic Matroids

Pradeep Sarvepalli*
Department of Physics and Astronomy, University of British Columbia, Vancouver, BC V6T 1Z1
(Dated: April 6, 2011)

The correspondence between linear codes and representable matroids is well known. But a similar correspondence between quantum codes and matroids is not known. We show that representable symplectic matroids over a finite field $\mathbb{F}_q$ correspond to $\mathbb{F}_q$-linear quantum codes. Although this connection is straightforward, it does not appear to have been made earlier in literature. The correspondence is made through isotropic subspaces. We also show that the popular Calderbank-Shor-Steane (CSS) codes are essentially the homogenous symplectic matroids while the graph states, which figure so prominently in measurement based quantum computation, correspond to a special class of symplectic matroids, namely Lagrangian matroids. This association is useful in that it enables the study of symplectic matroids in terms of quantum codes and vice versa. Furthermore, it has application in the study of quantum secret sharing schemes.

Keywords: quantum codes, symplectic matroids, Lagrangian matroids, graph states, quantum secret sharing, quantum cryptography

I. INTRODUCTION

Matroids are mathematical structures that abstract the idea of independence. Originally, introduced by Whitney, they have since found applications in various fields most notably in algorithms, combinatorial optimization, graphs, cryptography, coding theory to name a few. A particular class of matroids called the representable matroids are closely related to error-correcting codes. In fact, the so-called representations of these matroids give rise to linear codes; further, one can obtain matroids from linear codes. This correspondence goes much deeper in that certain invariants of the code are essentially invariants of the matroid as well. (Most well-known is the connection between the weight enumerator of a linear code and the Tutte polynomial of the matroid associated to the code.)

Given these associations one is tempted to ask if we can find a similar correspondence between quantum codes and (a class of) matroids? The answer to this question, as we shall see, is surprisingly simple and straightforward. In fact, it goes back to the many ways we can view matroids. But this connection does not appear to have made in the literature so far.

The main results of this paper are the correspondence between quantum codes and matroids, and applications of this correspondence. Strictly speaking we establish a correspondence between quantum codes and objects which are more general than matroids, called the symplectic matroids. Symplectic matroids generalize matroids, although their definition is somewhat more complicated than matroids. Our result has important applications. It can be used to study quantum codes using matroids and vice versa. We also find an application for these results in quantum secret sharing. We show how certain symplectic matroids induce quantum secret sharing schemes. There are many important open problems that arise with this connection and we are hopeful that further research along these lines will be fruitful for either communities of quantum information theorists and matroid theorists.

* pradeep@phas.ubc.ca

II. BACKGROUND

A. Symplectic matroids

Our presentation of the symplectic matroids follows the exposition in [1] very closely. Consider the sets $[n] = \{1,\ldots,n\}$ and $[n]^* = \{1^*,\ldots,n^*\}$. Let $J = [n] \cup [n]^*$ and define an involution on J as

$$* : J \to J, \text{ where } i \mapsto i^* \text{ and } (i^*)^* = i \tag{1}$$

This map can be extended naturally to subsets of J. A set $S \subset J$ is said to be admissible if $S \cap S^* = \emptyset$. A transversal is an admissible set of size n; it is a maximal admissible set. Consider now the group of permutations on the set J; a permutation is said to be admissible if it commutes with the involution. This group of admissible permutations on J, denoted as W, is the hyperoctahedral group of symmetries, the group of symmetries of the hypercube $[-1,1]^n$ in n-dimensions.

Consider the ordering of the elements of J as given by

$$n > n-1 > \cdots > 2 > 1 > 1^* > 2^* \cdots > n^*. \tag{2}$$

We now define another ordering on the set J by means of the admissible permutation $w \in W$. We say that $i \leq^w j$ if and only if $w^{-1}i \leq w^{-1}j$. Let w be given by the following permutation:

$$\begin{pmatrix} 1 & 2 & \ldots & n & n^* & \ldots & 2^* & 1^* \\ i_1 & i_2 & \ldots & i_n & i_{n+1} & \ldots & i_{2n-1} & i_{2n} \end{pmatrix}$$

This permutation induces the ordering $\prec$ given by

$$i_1 < i_2 < \cdots < i_n < i_{n+1} < \cdots < i_{2n}.$$

Clearly, $\prec$ induces an ordering on the subsets of J. It can also be used to order subsets $A, B \subset J$. Given two subsets $A = \{a_1,\ldots,a_m\}$, and $B = \{b_1,\ldots,b_m\}$, we say that $A \leq^w B$ if and only if $a_i \leq^w b_i$, where we assumed that A and B have been ordered as $\{a_1 \prec a_2 \prec \cdots \prec a_m\}$ and $\{b_1 \prec b_2 \prec \cdots \prec b_m\}$ respectively.

Definition 1 (Symplectic matroids)**.** *Let J_k be the collection of admissible k-subsets of J and $\mathcal{B} \subseteq J_k$. A tuple $(J, *, \mathcal{B})$*

is a symplectic matroid if and only if it satisfies the following condition:

For every admissible ordering of the set J, there exists a unique maximal set $B \in \mathcal{B}$ such that for all $A \in \mathcal{B}$, we have $A \prec B$.

The condition mentioned above is often called the ***Maximality condition***. The elements of $\mathcal{B}$ are called bases while $\mathcal{B}$ itself is called collection of the bases of the symplectic matroid. The cardinality of the bases is called is the rank of the matroid. (All the bases have the same size.) If the rank of the symplectic matroid is the maximal value of n, then it is said to be a Lagrangian matroid.

Remark 1. *Suppose we set $J = [n]$ and instead of W, we consider the symmetric group of all permutations, ie. all permutations on J are admissible. Then the tuple $(J, \mathcal{B})$, where $\mathcal{B}$ is a collection of k-subsets of J, is a matroid if and only if $\mathcal{B}$ satisfies the Maximality condition. In this case the involution plays no role. It is common in this case to refer to J as the ground set.*

B. Representable symplectic matroids

It is often convenient to deal with what are known are as the representations of a matroid. These representations provide us with a concrete object to work with and study the properties of the matroid. An ordinary matroid is said to have a representation if the elements of the ground set can be identified with the columns of a matrix (typically over some field) such that columns indexed by the bases are maximally linearly independent columns of that matrix.

Some symplectic matroids can also be endowed with representations. In this case instead of a standard vector space (with an orthogonal basis), we consider a symplectic vector space. That is a space of dimension $2n$ and endowed with a symplectic form $\langle \cdot, \cdot \rangle$, whose basis $\{e_1, \ldots, e_n, e_1^*, \ldots, e_n^*\}$ satisfies the following relations:

$$\langle e_i, e_j \rangle = 0, i \neq j^* \tag{3}$$

$$\langle e_i, e_i^* \rangle = -\langle e_i^*, e_i \rangle = 1 \tag{4}$$

Definition 2. *A vector space V over a field $\mathbb{F}$ is said to be isotropic if and only if for any $u, v \in V$ we have $\langle u, v \rangle = 0$, where $\langle \cdot, \cdot \rangle$ is the inner product.*

Let U be an isotropic subspace of a symplectic vector space. Suppose we write down a basis of this isotropic space as the rows of a matrix $M = [A|B] \in \mathbb{F}^{k \times 2n}$, where k is the dimension of V; then we must have $AB^t = BA^t$. Index the columns of M by the set $J = [n] \cup [n]^*$. Let $B \subset J$ such that $B \cap B^* = \emptyset$ and $|B| = k$. Then if the $k \times k$ minor of M indexed by B is nonzero, then we say that B is a basis of M. Let $\mathcal{B}$ denote the collection of bases of M. Then $(J, *, \mathcal{B})$ is a symplectic matroid over $\mathbb{F}$.

Proposition 1 ([1])**.** *Let the row space of $M = [A|B] \in \mathbb{F}^{s \times 2n}$ be an isotropic subspace with respect to a symplectic form. Then M is the representation of a symplectic matroid.*

A symplectic matroid is said to be homogenous if for every basis $B \in \mathcal{B}$, we have $|B \cap [n]|$ is same. For such a matroid $|B \cap [n]^*|$ is also independent of B. If such a matroid is representable then its representation is of the form

$$M = \begin{bmatrix} X & 0 \\ 0 & Z \end{bmatrix},$$

where $XZ^t = 0$. For the rest of the discussion in this paper we will assume that the matroid representations are over a finite field $\mathbb{F}_q$; occasionally we specialize to the case of $\mathbb{F}_2$ for simplicity.

III. CONNECTIONS WITH QUANTUM CODES

We recall some of the notions relevant for quantum codes. We will confine our discussion to additive quantum codes, in particular to stabilizer codes. Interested readers can find more details in [2, 3] for binary quantum codes and [4–7] for non-binary versions. Let q be the power of a prime p and $\mathbb{F}_q$ a finite field. Suppose that $\mathbb{C}^q$ denotes the q-dimensional complex vector space. Fix a basis for $\mathbb{C}^q$ as $B = \{|x\rangle \mid x \in \mathbb{F}_q\}$. We define error operators on $\mathbb{C}^q$ as $X(a)|x\rangle = |x + a\rangle$ and $Z(b)|x\rangle = \omega^{\mathrm{tr}_{q/p}(bx)}|x\rangle$. Error operators on n such q-level quantum systems are operators on $\mathbb{C}^{q^n}$ and are obtained as tensor products of the operators on $\mathbb{C}^q$. These error operators form the generalized Pauli group which is denoted as

$$\mathcal{P}_n = \{\omega^c X(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n)\}, \tag{5}$$

where $\omega = e^{j2\pi/p}$.

An $((n, K, d))_q$ quantum code is a K-dimensional subspace of the q^n-dimensional complex vector space $\mathbb{C}^{q^n}$ and able to detect all errors on fewer than d subsystems. When $K = q^k$, it is also denoted as an $[[n, k, d]]_q$ code. A stabilizer code is the joint eigenspace of an abelian subgroup of $\mathcal{P}_n$. The subgroup is called the stabilizer of the code. For a nontrivial quantum code, the stabilizer does not have any scalar multiple of identity other than the identity itself.

By defining a map between the Pauli group and the vector spaces over $\mathbb{F}_q^{2n}$, we can establish a correspondence between quantum codes and classical codes. This correspondence with the classical codes has been used extensively in the study of quantum codes [2–7]. An element $\omega^c X(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n)$ in $\mathcal{P}_n$ is mapped to $(a_1, \ldots, a_n|b_1, \ldots, b_n) \in \mathbb{F}_q^{2n}$. Under this mapping the stabilizer of the quantum code is mapped to a $\mathbb{F}_p$-linear subspace of $\mathbb{F}_q^{2n}$. If the image of the stabilizer is also an $\mathbb{F}_q$-linear subspace then we say that it is an $\mathbb{F}_q$-linear quantum code. In this paper we restrict our attention to $\mathbb{F}_q$-linear codes only. The image of a set of generators of the stabilizer under this map is often called a stabilizer matrix.

The relevant bilinear form that we endow $\mathbb{F}_q^{2n}$ with is the symplectic inner product defined as follows. Let u, v be two vectors in $\mathbb{F}_q^{2n}$ where $u = (a|b) = (a_1, \ldots, a_n|b_1, \ldots, b_n)$ and $v = (c|d) = (c_1, \ldots, c_n|d_1, \ldots, d_n)$. Then their symplectic inner product is defined as

$$\langle u|v \rangle_s = (a \cdot d - c \cdot b). \tag{6}$$

It is $\mathbb{F}_q$-linear in the sense that $\langle u|v\rangle_s = 0$ if and only if $\langle \alpha u|\beta v\rangle_s = 0$ for all $\alpha, \beta \in \mathbb{F}_q$. It can be easily checked that this form is asymmetric as $\langle u|v\rangle_s = -\langle v|u\rangle_s$. Denoting the standard basis of $\mathbb{F}_q^{2n}$ as $\{e_i, \ldots, e_n, e_1^*, \ldots, e_n^*\}$, we can check that $\langle e_i|e_j\rangle_s = 0$ for $i \neq j^*$, and $\langle e_i|e_i^*\rangle_s = 1$.

In this case the stabilizer matrix of an $\mathbb{F}_q$-linear $[[n,k,d]]_q$ quantum code defines an isotropic subspace of $\mathbb{F}_q^{2n}$ and is an element of $\mathbb{F}_q^{(n-k)\times 2n}$. This gives us the following result:

Proposition 2 ([2, 3])**.** *Let Q be an $[[n,k,d]]_q$ $\mathbb{F}_q$-linear quantum code, then the row space of the stabilizer matrix of the code defines an isotropic subspace of dimension $n-k$.*

Putting together with our discussion on the representations of symplectic matroids the following result is immediate.

Theorem 1. *Let Q be an $[[n,k,d]]_q$ $\mathbb{F}_q$-linear quantum code. Then Q induces a representable symplectic matroid over $\mathbb{F}_q$ of rank $n-k$. If Q is a CSS code it induces a representable homogenous matroid.*

Proof. This is an immediate consequence of Proposition 2 and Proposition 1. The stabilizer matrix of a CSS code is precisely the same form as in equation (11), (see [2]) and consequently, it induces a homogeneous symplectic matroid. □

It turns out the distance of the quantum code is related to the cardinality of the circuit of smallest size but to prove it more precisely we must wait till we have a few more results in hand.

With appropriate permutation of the columns of its representation a representable Lagrangian matroid can be put in the form $\begin{bmatrix} I & A \end{bmatrix}$, where A is a symmetric matrix. If A is such that its diagonal is all zero then we can identify it with adjacency matrix of a (weighted) graph. Recall that a graph state over $\mathbb{F}_2$ is defined as the quantum state whose stabilizer is given by

$$S = \left\langle K_v \mid v \in V(G); K_v = X_v \prod_{u\in N(v)} Z_u \right\rangle \qquad (7)$$

where $V(G)$ is the vertex set of G and $N(v)$ is the set of neighbors of v. If G is a weighted graph we can define a graph state over $\mathbb{F}_q$ with stabilizer as follows:

$$S = \left\langle K_v \mid v \in V(G); K_v = X_v(1) \prod_{u\in N(v)} Z_u(w_{uv}) \right\rangle \qquad (8)$$

where w_{uv} is the weight of the edge uv. See [8, 9] for more details on nonbinary graph states.

Since a stabilizer state corresponds to an $[[n,0,d]]_q$ code, Theorem 1 implies the following:

Corollary 2. *Every graph state induces a representable Lagrangian matroid.*

We pause to note a few differences with respect to the correspondence between matroids and classical codes. In case of classical codes the independent sets correspond to a subset of errors that are detectable. The codewords correspond to dependent sets. Further, the minimally dependent codewords characterize the matroid completely. (A minimal codeword x does not contain the support of any other codeword y, unless y is the scalar of x.) The supports of these minimal codewords are called circuits of the associated matroid. The concept of circuits can be generalized for symplectic matroids but circuits are most useful in the characterization of special cases of symplectic matroids such as Lagrangian matroids.

Classical (linear) codes have well-defined dual codes, on the other hand, there is no equivalent notion of a dual quantum code for a quantum code be it linear or additive. And not surprisingly, we find that a similar notion of duality is lacking for symplectic matroids. There has been a suggestion by Borovik [10] to use the involution defined in equation (1) for defining duals, however this suggestion seems to be most fruitful for the Lagrangian matroids and not for the general symplectic matroids.

Remark 2 (Quantum codes and ordinary matroids)**.** *Suppose that an $[[n,k,d]]_q$ quantum code is $\mathbb{F}_{q^2}$-linear, then we can also associate an ordinary matroid to that code in addition to a symplectic matroid. In this case the stabilizer matrix can be represented by a $(n-k)/2 \times n$ matrix over $\mathbb{F}_{q^2}$. In this particular instance, we can associate the vector matroid of this matrix to the quantum code. Thus $\mathbb{F}_{q^2}$-linear codes afford multiple associations to matroids.*

A. New quantum codes from graphical symplectic matroids

Quantum codes from graphs have been studied extensively in the context of fault tolerance. We now propose a new class of quantum codes induced by graphs by way of symplectic matroids. These are derived from the graphical symplectic matroids proposed by Chow [10].

The graphical symplectic matroids are defined as follows. Let G be a graph of n edges. Label the edges of the graph by a transversal $T \subset [n] \cup [n]^*$. (Recall that a transversal in an admissible set of size n.) A cycle in G is called balanced if there are an even number of edges labeled with elements from $[n]^*$, otherwise it is said to be unbalanced. An admissible set $S \subset [n] \cup [n]^*$ is an independent set if it is either a forest or every connected component is a tree plus an edge such that the cycle has an odd number of edges in $[n]^*$. It is the import of [10, Theorem 2], that the maximal independent sets form the bases of a symplectic matroid.

Assuming a connected graph, we can state some properties of these symplectic matroids. If the graph is a tree, then the rank of the symplectic matroid is $|V|-1$. If the graph is not a tree, then the rank is $|V|$. If these matroids are representable then we have a quantum code from Theorem 1. However, all graphic symplectic matroids are not representable [10]. Supposing that it is representable then the code has parameters $[[|E(G)|, |E(G)|-|V(G)|, d]]_q$, where $d \geq$ the smallest cycle in the graph.

As an example, the complete graph on three vertices is identical to the graph state on that graph. For dense graphs the associated codes are not likely to have good distance. On the other hand, sparse graphs might lead to good quantum

codes. The main reason for proposing these codes is to illustrate the possibility that matroids can provide new perspectives on quantum codes.

B. New symplectic matroids via quantum codes

Unlike matroids, symplectic matroids are a little more restricted in obtaining new symplectic matroids from existing ones. There are a however, few constructions known for constructing symplectic matroids: contraction, truncation, Higgs lift and direct sum [1]. For the representable symplectic matroids which correspond to $\mathbb{F}_q$-linear quantum codes one can relate these constructions to familiar coding theoretic operations.

Consider a symplectic matroid of rank k whose collection of bases are given by $\mathcal{B}$. Contraction (along) $a \in J$ is defined by the following operation:

$$\mathcal{B}' = \{B \mid (B \cup \{a\}) \in \mathcal{B}\}, \tag{9}$$

where $\mathcal{B}'$ is the collection of bases of the resulting symplectic matroid. This translates to obtaining an $[[n-1, k]]_q$ from an $[[n, k]]_q$ code. Truncation modifies $\mathcal{B}$ as

$$\mathcal{B}' = \{A \in J_{k-1} \mid A \subset B \in \mathcal{B}\}. \tag{10}$$

In coding theoretic terms this is equivalent to obtaining an $[[n, n-k+1]]_q$ quantum code from an $[[n, n-k]]_q$ quantum code.

On the other hand deletion corresponds to puncturing on the underlying code and as this does not always preserve a self-orthogonality of the code, this construction does not generalize. An interesting method for constructing new symplectic matroids is the so-called Higgs lift [1]. This corresponds to obtaining an $[[n, k-1]]_q$ code from an $[[n, k]]_q$ code.

Two symplectic matroids can be combined to give rise to a third matroid in many ways. The simplest method is the direct sum method. Concatenation is a popular method to construct new codes and if done appropriately it gives rise to another self-orthogonal code. There are many flavors of concatenating quantum codes [4, 11]. These constructions can be translated to equivalent constructions of symplectic matroids.

C. Transformations of symplectic matroids

One of the most studied equivalence of quantum codes is local equivalence, especially local Clifford equivalence. It is natural to ask if this corresponds to any equivalence on the associated symplectic matroids. The (representable) symplectic matroids are not going to be preserved under local Clifford operations in general. This can be checked with the complete graph on 3 vertices and the graph obtained by local complementation at any of the vertices. The symplectic matroid associated with the line graph on 3 vertices has the representation

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

with the associated bases being $\{\{1,2,3\},\{1^*,2^*,3\},\{1^*,2,3^*\}\}$ On the other hand, the symplectic matroid of graph state on the complete graph on three vertices which is local Clifford equivalent to it has the representation

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

This symplectic matroid has its collection of bases $\{\{1,2,3\},\{1^*,2^*,3\},\{1^*,2,3^*\},\{1,2^*,3^*\}\}$. This prompts the question is there an operation by which we can express this transformation of the symplectic matroid in terms of an operation on its bases?

One of the methods to obtain an equivalent symplectic matroid is via the torus action defined as follows. Let $[A|B]$ be the representation of a symplectic matroid. Then for any invertible $n \times n$ diagonal matrix T, the representation $[AT^{-1}|BT]$ is also a representation of the symplectic matroid. The torus action gives rise to an equivalent quantum code with the same parameters. Furthermore, the weight distribution of the code is unchanged under the torus action.

D. Representable homogeneous symplectic matroids

Given a symplectic matroid define a circuit to be a minimally dependent admissible subset of J. Then we have the following characterization for the homogenous symplectic matroids. These results will be needed later in the section on quantum secret sharing.

Lemma 3. *Every circuit of a representable homogeneous symplectic matroid consists of either elements in $[n]$ or $[n]^*$.*

Proof. Suppose that there is a minimally dependent admissible set $C \subset J$ such that $C \cap [n] \neq \emptyset$ and $C \cap [n]^* \neq \emptyset$. Without loss of generality assume that $C = \{1, \ldots, m, (m+1)^*, \ldots, p^*\}$. Assume that the representation of the symplectic matroid is given by

$$M = \left[\begin{array}{c|c} X & 0 \\ 0 & Z \end{array}\right]. \tag{11}$$

As C is a circuit, there exists a linear combination of the columns $\{1, \ldots, m\}$ and the columns $\{(m+1)^*, \ldots, p^*\}$. However given the fact that the representation of the matroid is of the form equation (11), the columns $\{1, \ldots, m\}$ and $\{(m+1)^*, \ldots, p^*\}$ are linearly dependent as well. But this implies that C is not a minimally dependent set. Therefore every circuit of the homogenous symplectic matroid is either a subset of $[n]$ or $[n]^*$ but not both. □

Theorem 4. *Representable homogenous symplectic matroids, satisfy the Circuit elimination property: If C_1, $C_2 \in \mathcal{C}$, such that $e \in C_1 \cap C_2$ and $C_1 \cup C_2$ is admissible, then there exists a circuit $C \in \mathcal{C}$ such that $C \subseteq (C_1 \cup C_2) \setminus \{e\}$.*

Proof. Let C_1 and C_2 be two circuits of $\mathcal{M}$. By Lemma 3, every such circuit consists of elements in $[n]$ or $[n]^*$. Suppose that $C_1 \cap C_2 \neq \emptyset$. Then this is possible if and only if both $C_1, C_2 \subset [n]$ or $C_1, C_2 \subset [n]^*$. Without loss of generality assume that $C_1, C_2 \subset [n]$. Let $e \in C_1 \cap C_2$. Then e can be expressed a linear combination of columns in $C_1 \setminus \{e\}$ as well as $C_2 \setminus \{e\}$. It is then immediate that $C_1 \cup_2 \setminus \{e\}$ is a dependent set and must contain a minimal dependent set equivalently a circuit in $[n]$, which is clearly an admissible set. Thus representable homogenous symplectic matroids satisfy the circuit elimination property. □

Before we move to some applications of these results, we raise the question we address the issue of invariants for the symplectic matroids.

E. Invariants for symplectic matroids

An important invariant associated with matroids is the rank polynomial. As a weight enumerator captures many of the invariants of the code (such as distance), the rank polynomial encodes information about many invariants of the matroids. The rank polynomial has been related to other polynomials of interest such as Tutte polynomial of a graph, the Kauffman polynomial of a knot, the partition function and has been studied extensively in view of its relevance to complexity theory. But from a coding theoretic point of view the weight enumerator and the rank polynomial are closely related. All this brings up the question if there are similar polynomials for the symplectic matroids which are of interest to quantum codes. A general answer to this question eludes us, but when we focus our attention to the Lagrangian matroids, we can partially answer this question.

In [12], Bouchet studied graph polynomials for isotropic systems that are related to the Tutte polynomial of an associated graph. Isotropic systems are essentially Lagrangian matroids. Consequently the following Tutte-Martin polynomials as defined by Bouchet are only defined for Lagrangian matroids.

Definition 3 (Restricted Tutte-Martin polynomial)**.** *Let L be a Lagrangian matroid. Define the restricted Tutte-Martin polynomial as*

$$m(L;x) = \sum_{S \in J_n} (x-1)^{n-\mathrm{rk}(S)}. \tag{12}$$

where $n = \mathrm{rk}(L)$.

We could attempt to define a similar polynomial for symplectic matroids that are not Lagrangian. For a symplectic matroid, L we define the restricted Tutte-Martin polynomial as

$$m(L;x) = \sum_{S \in J_k} (x-1)^{k-\mathrm{rk}(S)}. \tag{13}$$

where $k = \mathrm{rk}(L)$.

Suppose M is a representable Lagrangian matroid, with representation $[I|A]$, for some symmetric matrix, A. Then its restricted Tutte-Martin polynomial is the same as the interlace polynomial of a graph G with adjacency matrix A. Note that the interlace polynomial $q_N(x)$ is defined as [13]

$$q_N(G;x) = \sum_{S \subseteq V(G)} (x-1)^{\mathrm{corank}(G(S))}, \tag{14}$$

where $G(S)$ is the subgraph of G induced by S. Bouchet who originally defined the restricted Tutte-Martin polynomial gave it in a slightly different form.

Recent work [14] has made the connection between interlace polynomial and orbits of quantum states and codes under edge local complementation. Perhaps the most famous polynomial associated to matroids is the rank polynomial or the Tutte polynomial. It does not seem possible to define a Tutte polynomial for a symplectic matroid in general and might require an expansion of the definition of symplectic matroid.

IV. APPLICATION FOR QUANTUM SECRET SHARING

In [15], connections between matroids and quantum secret sharing schemes were investigated. It was shown that identically self-dual matroids induce quantum secret sharing schemes thereby this establishing a connection between matroids and quantum secret sharing schemes. However, it was somewhat limited in that only quantum secret sharing schemes that are realized using a CSS code were within that correspondence. In present section we intend to make this matroidal correspondence stronger by including a larger class of schemes some of which can be realized by non-CSS codes.

Given a Lagrangian matroid L whose collection of bases is $\mathcal{B}$, we can define the dual matroid as follows. The collection of bases of the dual matroid are given by $B^* = \{B^* \mid B \in \mathcal{B}\}$. Similarly, the collection of circuits of the dual matroid are given by $\mathcal{C}^* = \{C^* \mid C \in \mathcal{C}\}$. Elements of $\mathcal{C}^*$ are also called cocircuits of $\mathcal{L}$.

Let L be a self-dual Lagrangian matroid, then we define an access structure from the circuits of $\mathcal{L}$ as follows. Define the map $\varphi : [n] \cup [n]^* \to [n]$ where

$$\varphi(i) = \begin{cases} i & \text{if } i \in [n] \\ i^* & \text{if } i \in [n]^* \end{cases} \tag{15}$$

We obtain an access structure by considering $i \in [n]$ as the dealer. The induced minimal access structure is given as

$$\Gamma_{i,\min} = \{\varphi(A) \mid A \cup \{i\} \text{ or } A \cup \{i^*\} \in \mathcal{C}\}, \tag{16}$$

where $\mathcal{C}$ is the collection of circuits of $\mathcal{L}$. We say a Lagrangian matroid is secret sharing if the access structure induced by it for any $i \in [n]$ is a quantum access structure. (Such an access structure is monotonic and satisfies the no-cloning theorem. In terms of minimal access structures, it means that any two authorized sets are not disjoint.)

It is possible that a Lagrangian matroid can induce a quantum access structure for some $i \in [n]$ but not all i. For simplicity we consider the case when it induces on all $i \in [n]$.

We do not yet have a condition for which Lagrangian matroids induce quantum access structures and which do not.

We provide partial answers in both directions. First we give a necessary condition for a Lagrangian matroid to induce a quantum secret sharing scheme. Then we give a sufficient condition for a Lagrangian matroid to induce a secret sharing scheme.

Theorem 5. *Suppose that G is a graph wihtout loops or multi-edges and whose adjacency matrix is given by A. Let L be a Lagrangian matroid induced by G such that L is represented by $\left[\begin{array}{cc} I & A \end{array}\right]$. If G has no cycles of length ≤ 4 and no vertices of degree 1, then the access structure induced by L is not a valid quantum access structure.*

Proof. A Lagrangian matroid of this type corresponds to a graph state whose stabilizer is given by

$$S = \langle K_v \mid v \in V(G) \rangle \text{, where } K_v = X_v \prod_{i \in N(v)} Z_i$$

and $V(G)$ is the vertex set of G and $N(v)$ is the set of neighbors of v. The associated Lagrangian matroid has the representation $\left[\begin{array}{cc} I & A \end{array}\right]$. Consider access structure induced by the vertex v.

$$\Gamma_{v,\min} = \{\varphi(A) \mid A \cup \{v\} \text{ or } A \cup \{v^*\} \in \mathcal{C}\}.$$

Of interest are two elements in $\mathcal{C}$ that are induced by the generators K_u, where $u, w \in N(v)$. By assumption $|N(v)| > 1$. Therefore there are at least two generators $u, w \in N(v)$. The supports of generators correspond to circuits and are of the $\{u\} \cup N(u)^*$ and $\{w\} \cup N(w)^*$ respectively. Consequently the sets induced by these circuits are of the form $\operatorname{supp}(K_u) \setminus \{v\}$ and $\operatorname{supp}(K_w) \setminus v$. We claim that these two sets are disjoint. Suppose that they are not, then there exists a vertex $x \neq v$ such that $x \in \operatorname{supp}(K_u) \cap \operatorname{supp}(K_w)$. This implies that G has a 4-cycle contrary to assumptions. Therefore these two circuits induce disjoint authorized sets and the induced access structure cannot be a quantum access structure. □

Lemma 6. *Let L be a self-dual Lagrangian matroid whose collection of circuits is given by $\mathcal{C}$. Then the collection of cocircuits of L is given by $\mathcal{C}^* = \{C^* \mid C \in \mathcal{C}\} = \mathcal{C}$.*

Proof. Let $\mathcal{B}$ be the collection of bases of the matroid. Then collection of bases of the dual matroid is given by $\mathcal{B}^* = \{B^* \mid B \in \mathcal{B}\}$. Let $C \in \mathcal{C}$ be a circuit of the matroid. Since B^* is also an element of $\mathcal{B}$, C is not a subset of B^* for any $B \in \mathcal{B}$. Therefore, C^* is in $\mathcal{C}$ as well, and $\mathcal{C} = \mathcal{C}^* = \{C^* \mid C \in \mathcal{C}\}$, which is precisely the collection of circuits of the dual matroid. □

Theorem 7. *Let $\mathcal{L}$ be a self-dual Lagrangian matroid. Then the access structure $\Gamma_{i,\min}$ as defined in equation* (16) *is a valid quantum access structure.*

Proof. Let A' and B' be two authorized sets in $\Gamma_{i,\min}$. Then there exist two circuits $A \cup \{a\}$ and $B \cup \{b\}$ such that $A' = \varphi(A)$ and $B' = \varphi(B)$, where $a, b \in \{i, i^*\}$. Suppose that $a \neq b$. We observe that $B^* \cup \{b^*\}$ must be a cocircuit of $\mathcal{L}$. Since $\mathcal{L}$ is self-dual it follows that $B^* \cup \{b^*\}$ is a circuit of $\mathcal{L}$. Since $\varphi(B) = \varphi(B^*)$, we can instead consider B^*. Without loss of generality we can assume that $a = b = i$.

The self-duality of $\mathcal{L}$ implies that $B \cup \{i\}$ is a cocircuit of $\mathcal{L}$. By [1, Theorem 4.2.5] it follows that

$$|(A \cup \{i\}) \cap (B \cup \{i\})| \neq 1.$$

But this implies that $|A \cap B| \geq 1$ for any pair of minimal authorized sets. This is the necessary and sufficient condition for an access structure to be a minimal quantum access structure. □

Corollary 8. *A self-dual Lagrangian matroid induces a quantum secret sharing scheme.*

However, self-dual Lagrangian matroids are not the only matroids which induce valid quantum access structures. Consider the Lagrangian matroid whose representation is given by the following matrix.

$$\left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

The circuits of this matroid are given by

$$\mathcal{C} = \left\{ \begin{array}{c} \{1, 3^*, 4, 5^*\}, \{1, 4^*, 5, 6^*\}, \{1, 2^*, 5^*, 6\}, \\ \{1, 2, 3^*, 6^*\}, \{1, 2^*, 3, 4^*\}, \{1^*, 2^*, 4, 5\}, \\ \{1^*, 3^*, 5, 6\}, \{1^*, 2, 4^*, 6\}, \{1^*, 2, 3, 5^*\}, \\ \{1^*, 3, 4, 6^*\}, \{2, 3^*, 4^*, 5\}, \{3, 4^*, 5^*, 6\}, \\ \{2, 4, 5^*, 6^*\}, \{2^*, 3, 5, 6^*\}, \{2^*, 3^*, 4, 6\} \end{array} \right\}$$

The access structure induced by the treating the first coordinate as the dealer is given by

$$\Gamma_{1,\min} = \left\{ \begin{array}{c} \{2, 3, 4\}, \{2, 3, 5\}, \{2, 3, 6\}, \{2, 4, 5\}, \\ \{2, 4, 6\}, \{2, 5, 6\}, \{3, 4, 5\}, \{3, 4, 6\}, \\ \{3, 5, 6\}, \{4, 5, 6\} \end{array} \right\}$$

This is precisely the access structure of the $((3, 5))$ threshold scheme and it can be realized using the $[[5, 1, 3]]$ code. As this matroid is not self-dual, it shows that class of matroidal quantum secret sharing schemes is strictly larger than the class induced by the class of self-dual Lagrangian matroids.

The dual of a matroid $M = (J, \mathcal{B})$ is given by $M^* = (J, \mathcal{B}^*)$, where $\mathcal{B}^* = \{J \setminus B \mid B \in \mathcal{B}\}$. A matroid is said to be identically self-dual if $M = M^*$. In [15], it was shown how to construct quantum secret sharing schemes from indentically self-dual matroids. This construction is a special case of Theorem 7.

Lemma 9. *Let M be an identically self-dual matroid. Then there exists a self-dual Lagrangian matroid L whose collection of bases is given by $\mathcal{B}(L) = \{B \cup ([n] \setminus B)^* \mid B \in \mathcal{B}(M)\}$. Further L induces the same quantum access structure as M.*

Proof. To see this consider a identically self-dual matroid M whose collection of bases is given by $\mathcal{B}_1$. The collection of the bases for the dual matroid are given by $\mathcal{B}_1^\perp = \mathcal{B}_1$ because M is identically self-dual. By definition $\mathcal{B}_1^\perp = \{[n] \setminus B \mid B \in \mathcal{B}_1\}$. Therefore, for every basis B, $[n] \setminus B$ is also in $\mathcal{B}$. Now consider

forming a Lagrangian matroid whose collection of bases is given by $\mathcal{B} = \{B \cup ([n] \setminus B)^*\}$. It is Lagrangian because the cardinality of any element in $\mathcal{B}$ is n. The self-duality of the symplectic matroid is a consequence of the self-duality of M.

By Theorem 7, the access structure induced by L is a valid quantum access structure. We want to show that this access structure is precisely the access structure induced by the matroid M. Recall that the access structure induced by M is given by

$$\Gamma^M_{i,\min} = \{A \mid A \cup \{i\} \in \mathcal{C}(M)\},$$

where $\mathcal{C}(M)$ is the collection of circuits of M.

By Lemma 3, the circuits of L are either in $[n]$ or $[n]^*$. The restriction of L to the transversal $[n]$ gives the matroid M, while the restriction to $[n]^*$ gives the identically self-dual matroid $M^* = M$. Every circuit of L contained in the restriction $[n]$ (resp. $[n]^*$) is a circuit of M (resp. M^*). But these exhaust the circuits of L. Thus the access structure induced by L, as given in (16), is exactly the same access structure as M. □

V. CONCLUSION AND OPEN QUESTIONS

In this paper we have established a connection between quantum codes and symplectic matroids. This opens a new perspective on quantum codes and has potential applications for quantum cryptography. Furthermore, this correspondence raises a number of interesting questions that are worth pursuing. We list some of them here.

1) Find representations for the graphical symplectic matroids. Alternatively, find a criterion to test which of these matroids are representable.

2) Find out if the quantum codes derived from the symplectic matroid of a simple connected graph, have good parameters.

3) What are the necessary and sufficient conditions for Lagrangian matroids to induce quantum access structures? Can these be stated in terms of the graph underlying the Lagrangian matroid?

4) Given a secret sharing Lagrangian matroid, what is the associated quantum code that realizes this access structure?

5) Define a polynomial that captures the weight enumerator of the underlying quantum code for representable symplectic matroids.

We hope that the results in this paper will prompt further research into the applications of matroids for quantum information.

ACKNOWLEDGMENT

I would like to thank Robert Raussendorf for many helpful discussions, and his support and encouragement throughout this project. This research was sponsored by grants from NSERC, CIFAR, and MITACS.

[1] A. V. Borovik, I. M. Gelfand, and N. White, *Coxeter Matroids* (Birkhäuser, Boston, 2003).
[2] A. Calderbank, E. Rains, P. Shor, and N. Sloane, IEEE Trans. Inform. Theory **44**, 1369 (1998).
[3] D. Gottesman, "Stabilizer codes and quantum error correction," (1997), caltech Ph. D. Thesis, eprint: quant-ph/9705052.
[4] E. Rains, IEEE Trans. Inform. Theory **45**, 1827 (1999).
[5] A. Ashikhmin and E. Knill, IEEE Trans. Inform. Theory **47**, 3065 (2001).
[6] M. Grassl, M. Rötteler, and T. Beth, Internat. J. Found. Comput. Sci. **14**, 757 (2003).
[7] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inform. Theory **52**, 4892 (2006).
[8] D. Schlingemann and R. Werner, "Quantum error-correcting codes associated with graphs," (2000), eprint: quant-ph/00012111.
[9] M. Bahramgiri and S. Beigi, "Graph states under the action of local clifford group in non-binary case," (2007), arXiv:quant-ph/0610267v2.
[10] T. Chow, Discrete Mathematics **263**, 35 (2003).
[11] M. Grassl and M. Rötteler, in *Proc. 2005 IEEE Intl. Symposium on Information Theory, Adelaide, Australia* (2005) pp. 1018–1022.
[12] A. Bouchet, Discrete Mathematics **302**, 32 (2005).
[13] M. Aigner and H. van der Holst, Linear Algebra Appl. **377**, 11 (2004).
[14] L. E. Danielsen and M. G. Parker, Discrete Appl. Math. **158**, 636 (March 2010), ISSN 0166-218X.
[15] P. Sarvepalli and R. Raussendorf, Phys. Rev. A **81** (2010).